PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-154139
(43)Date of publication of application : 08.06.1999

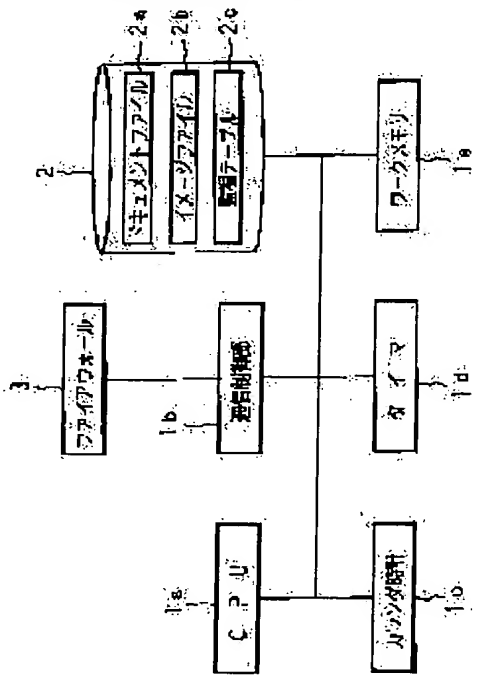
(51)Int.Cl. G06F 15/00
G06F 11/30
G06F 12/14
G06F 13/00

(21)Application number : 09-318718
(22)Date of filing : 19.11.1997

(71)Applicant : FUJITSU LTD
(72)Inventor : ISHIBASHI JUNJI

(54) METHOD AND DEVICE FOR CORRECTING FORGERY AND FORGERY DISCRIMINATING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To suppress the expansion of a damage scale caused by the forged contents.
SOLUTION: After the elapse of prescribed time, the contents of a monitoring object are acquired from the location registered in a monitor table 2c and when the updated date of contents is not coincident with that of registered contents or when the size is not similarly coincident and further when contents are not coincident, the contents registered in a storage device 2, namely, a document file 2a and an image file 2b are disclosed to the said location. Then, electronic mail for reporting the execution of correction is transmitted to the user related to the preparation and management of these contents.



LEGAL STATUS

[Date of request for examination]	29.09.2000
[Date of sending the examiner's decision of rejection]	24.06.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3484523
[Date of registration]	24.10.2003
[Number of appeal against examiner's decision of rejection]	2003-014211
[Date of requesting appeal against examiner's decision of rejection]	24.07.2003
[Date of extinction of right]	

B2

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－154139

(43)公開日　平成11年(1999)６月８日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ
	11/30	３２０		11/30	３２０Ｃ
	12/14	３１０		12/14	３１０Ｚ
	13/00	３５１		13/00	３５１Ｚ

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平9－318718

(22)出願日　平成９年(1997)11月19日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　石橋　淳司
徳島県徳島市寺島本町西一丁目７番地１
株式会社富士通徳島システムエンジニアリング内

(74)代理人　弁理士　河野　登夫

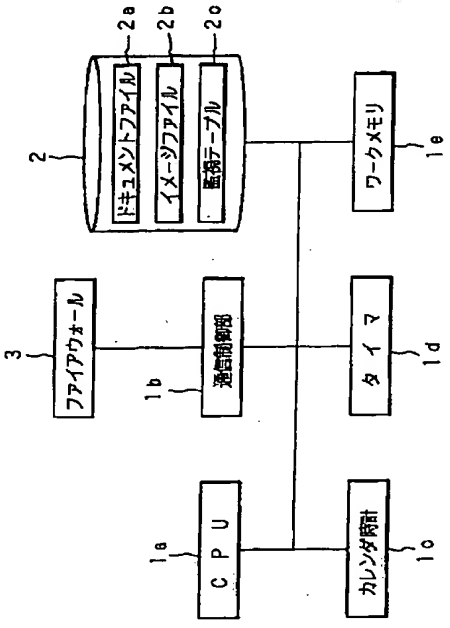
(54)【発明の名称】　改竄修正方法，改竄修正装置及び改竄判定装置

(57)【要約】

【課題】　コンテンツの改竄による被害規模の拡大を抑止する。

【解決手段】　所定の経過時間に達したとき、監視テーブル2cに登録されたロケーションから監視対象のコンテンツを入手して、該コンテンツの更新日付が登録されたコンテンツのそれと一致しないとき、また同様にサイズが一致しないとき、更にまた内容が一致しないとき、記憶装置２に登録されているコンテンツ、即ちドキュメントファイル2a及びイメージファイル2bを前記ロケーションへ開示する。そして、そのコンテンツの作成及び管理に関係するユーザへ、修正を行ったことを通知する電子メールを発信する。

本発明に係る改竄修正装置の構成を示すブロック図



【特許請求の範囲】
【請求項１】　ネットワーク上の所定のロケーションで開示されているコンテンツを定期的に入手して、その都度前記コンテンツの内容が改竄されているか否かを判定し、改竄されたと判定したとき、元の内容に修正することを特徴とする改竄修正方法。
【請求項２】　ネットワーク上の所定のロケーションで開示されているコンテンツを定期的に入手して、その都度前記コンテンツの内容が改竄されているか否かを判定し、改竄されたと判定したとき、元の内容に修正する改竄修正装置であって、
開示すべきコンテンツの複製を格納する記憶手段と、
ネットワークとの接続を制御し、予め定められたタイミングで、前記ネットワーク上の所定のロケーションからコンテンツを入手するコンテンツ入手手段と、
入手したコンテンツと前記記憶手段に格納してあるコンテンツの複製とが一致するか否かに基づき改竄判定を行う判定手段と、
一致しないと判定したとき、前記記憶手段に格納してあるコンテンツの複製を前記ロケーションへ開示する開示手段とを備えることを特徴とする改竄修正装置。
【請求項３】　コンテンツのデータの特徴を抽出する抽出手段を備え、前記判定手段は、前記抽出手段により夫々抽出された前記記憶手段に格納してあるコンテンツの複製データの特徴と前記コンテンツ入手手段により入手したコンテンツのデータの特徴とが一致するか否かに基づき改竄判定を行うべくなしたことを特徴とする請求項２記載の改竄修正装置。
【請求項４】　ネットワーク上の所定のロケーションで開示されているコンテンツを定期的に入手して、その都度前記コンテンツの内容が改竄されているか否かを判定する改竄判定装置であって、
コンテンツのデータの特徴を抽出する抽出手段と、
該抽出手段により抽出された開示すべきコンテンツのデータの特徴を記憶する記憶手段と、
ネットワークとの接続を制御し、予め定められたタイミングで、前記ネットワーク上の所定のロケーションからコンテンツを入手するコンテンツ入手手段と、
該コンテンツ入手手段により入手したコンテンツのデータの特徴を前記抽出手段により抽出し、抽出したデータの特徴と前記記憶手段に格納してある開示すべきコンテンツのデータの特徴とが一致するか否かに基づき改竄判定を行う判定手段とを備えることを特徴とする改竄判定装置。
【請求項５】　前記記憶手段は、開示すべきコンテンツのデータの特徴と共に前記コンテンツの複製を格納し、前記判定手段により一致しないと判定したとき、前記記憶手段に格納してあるコンテンツの複製を前記ロケーションへ開示する開示手段を備えることを特徴とする請求項４記載の改竄判定装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークにおいて公開されたコンテンツが改竄されているか否かを定期的に監視して、改竄されたと判定されたとき、元の内容に修正することができる改竄修正装置及びその判定を行う改竄判定装置に関する。
【０００２】
【従来の技術】ネットワークを介して多数のユーザが利用可能なコンピュータシステムにおいては、ファイルの作成又は管理に関係するユーザではなく、他のユーザによってその内容の改竄が行われる可能性を有している。通常、前述の如きコンピュータシステムは、各ユーザに対して唯一つ対応するパスワードを予め設定しておき、該パスワードに基づき情報の開示範囲等を制限することによってファイルのアクセス権の保護を実現しており、改竄操作に対するセキュリティもこの仕組みに依存する。
【０００３】具体的には、コンピュータシステムのサーバコンピュータに各ユーザのログイン名及びそれに対応するパスワードを予め登録しておき、これらを対応する各ユーザへ通知しておく。また、前記サーバコンピュータに各ユーザの使用可能コマンド及びファイルの開示範囲を予め設定しておく。そして、コンピュータシステム（サーバコンピュータ）へのログイン時にユーザが入力したログイン名とパスワードが、予め登録してあるものと一致するか否かを判別し、一致するときユーザを識別して、使用コマンドの制限及びファイルの開示制限を行う。
【０００４】ところで、ファイルの作成又は管理に関係するユーザ、即ち情報提供者のパスワードが他のユーザに察知される可能性は存在する。他のユーザ、即ち不当なユーザは前記パスワードを察知したとき、それを使用して当人に成りすまし、ファイルの内容を改竄することができる。しかし、ファイルの内容の改竄操作が行われた場合に、前記情報提供者へその事実を通知する手段は用意されていない。従って、他のユーザによる改竄操作が行われたことを関知するためには、情報提供者自身による監視操作が必要である。以下にその概略を説明する。
【０００５】各ファイルには、その内容の更新日付及びそのサイズを表す情報が記録されており、これらの情報がファイルの内容の改竄操作が行われたことを関知するための手掛かりとなる。即ち、情報提供者はファイルの更新日付又はそのサイズの変化を発見した場合、自分が過去に行ったファイル操作の記憶と照合する。そして、記憶と一致しないとき、他のユーザによる改竄操作が行われたことを関知する。
【０００６】ところが、ファイルの更新日付の情報は、ファイルの内容と同様にして記録媒体に記録されている

ものである。従って、ファイルの内容を改竄した上で、その更新日付を元の日付に修正しておくことも不可能ではなく、しかもその改竄操作によってファイルのサイズが変化しない場合、前述のような手法に基づいて改竄操作が行われたことを関知することはできない。結局、このような状況に対処するために、情報提供者はファイルの内容の変更が有るか否かを、実際に閲覧して逐一検査しなければならない。そして内容の変更を発見した場合、過去に行った編集操作の記憶と照合し、記憶と一致しないとき、他のユーザによる改竄操作が行われたことを関知する。

【０００７】

【発明が解決しようとする課題】内容を改竄されたファイルが例えば、インターネットにアップロードされたコンテンツ等、多数のユーザに対して開示される情報を格納したものである場合、その改竄によって情報提供者の利益阻害又は名誉毀損が生じる可能性がある。しかも、その被害の規模は改竄操作が行われてから修正されるまでの期間に応じて拡大することが予想される。

【０００８】改竄による被害規模の拡大抑止のためには、定期的に監視操作を実施することが考えられる。しかし、前述の如き監視操作の定期的な実施は、情報提供者に多大な負担を強いることになり、現実的ではない。また、実際に情報提供者が他のユーザによる改竄操作が行われたことを関知したとき、情報提供者自身が当該部分を元の状態に修正操作することになるが、このような修正操作は簡素化されることが望ましい。

【０００９】本発明は、斯かる事情に鑑みてなされたものであって、ファイルの内容の改竄操作が行われたか否かを定期的に監視して、改竄操作が行われたことを関知したときに、速やかに当該部分を元の状態に修正することによって、改竄による被害規模の拡大を抑止することができる改竄修正装置，改竄修正方法及びその改竄操作有無の判定を行う改竄判定装置の提供を目的とする。

【００１０】

【課題を解決するための手段】第１発明に係る改竄修正方法は、ネットワーク上の所定のロケーションで開示されているコンテンツを定期的に入手して、その都度前記コンテンツの内容が改竄されているか否かを判定し、改竄されたと判定したとき、元の内容に修正することを特徴とする。

【００１１】第２発明に係る改竄修正装置は、ネットワーク上の所定のロケーションで開示されているコンテンツを定期的に入手して、その都度前記コンテンツの内容が改竄されているか否かを判定し、改竄されたと判定したとき、元の内容に修正する改竄修正装置であって、開示すべきコンテンツの複製を格納する記憶手段と、ネットワークとの接続を制御し、予め定められたタイミングで、前記ネットワーク上の所定のロケーションからコンテンツを入手するコンテンツ入手手段と、入手したコンテンツと前記記憶手段に格納してあるコンテンツの複製とが一致するか否かに基づき改竄判定を行う判定手段と、一致しないと判定したとき、前記記憶手段に格納してあるコンテンツの複製を前記ロケーションへ開示する開示手段とを備えることを特徴とする。

【００１２】第３発明に係る改竄修正装置は、コンテンツのデータの特徴を抽出する抽出手段を備え、前記判定手段は、前記抽出手段により夫々抽出された前記記憶手段に格納してあるコンテンツの複製データの特徴と前記コンテンツ入手手段により入手したコンテンツのデータの特徴とが一致するか否かに基づき改竄判定を行うべくなしたことを特徴とする。

【００１３】第４発明に係る改竄判定装置は、ネットワーク上の所定のロケーションで開示されているコンテンツを定期的に入手して、その都度前記コンテンツの内容が改竄されているか否かを判定する改竄判定装置であって、コンテンツのデータの特徴を抽出する抽出手段と、該抽出手段により抽出された開示すべきコンテンツのデータの特徴を記憶する記憶手段と、ネットワークとの接続を制御し、予め定められたタイミングで、前記ネットワーク上の所定のロケーションからコンテンツを入手するコンテンツ入手手段と、該コンテンツ入手手段により入手したコンテンツのデータの特徴を前記抽出手段により抽出し、抽出したデータの特徴と前記記憶手段に格納してある開示すべきコンテンツのデータの特徴とが一致するか否かに基づき改竄判定を行う判定手段とを備えることを特徴とする。

【００１４】第５発明に係る改竄判定装置は、前記記憶手段は、開示すべきコンテンツのデータの特徴と共に前記コンテンツの複製を格納し、前記判定手段により一致しないと判定したとき、前記記憶手段に格納してあるコンテンツの複製を前記ロケーションへ開示する開示手段を備えることを特徴とする。

【００１５】図４は、前述の改竄修正装置を使用した改竄修正の概念を説明する説明図である。図において、１は改竄修正装置の実施に使用するサーバコンピュータであって、ハードディスクドライブ等を用いてなる記憶装置２と接続している。また、サーバコンピュータ１は外部からの不正なアクセスを防ぐファイアウォール３を介してインターネット４と接続している。そして、WWW（World Wide Web）サーバとして機能する。記憶装置２には、内容の改竄が行われたときに修正すべきコンテンツの複製、具体的にはHTML（Hyper Text Markup Language）によって作成されたドキュメントファイル及びその内容において関連付けられているイメージファイルが格納される。また、その改竄判定に使用する監視テーブルが格納される。監視テーブルは、コンテンツの識別名，記憶装置２への登録（格納）日時，開示先のロケーション及び改竄判定を行った時刻を対応付けて作成される。

【００１６】一方、５はコンテンツの供給元のサーバコ

ンピュータであって、記憶装置６及びクライアントコンピュータ７，８，９と接続しており、これらはLAN（LocalArea Network）を形成する。また、サーバコンピュータ５はファイアウォール10を介してインターネット４と接続している。そして、WWW サーバとして機能する。記憶装置６には、他の記憶装置へ公開されているコンテンツの原本、即ちHTMLによるドキュメントファイル及びその内容において関連付けられているイメージファイルが格納される。

【００１７】また一方、11はコンテンツの開示先のロケーションのサーバコンピュータであって、記憶装置12と接続している。また、サーバコンピュータ11はファイアウォール13を介してインターネット４と接続している。更にまた、公衆回線網14と接続しており、クライアントコンピュータ15，16，17からのダイヤルアップIP接続を可能になしてあって、WWW サーバとして機能する。記憶装置12には、公開されているコンテンツ、即ちHTMLによるドキュメントファイル及びその内容において関連付けられているイメージファイルが格納される。

【００１８】以下に、改竄修正装置の使用に係るコンテンツの公開手順及びその内容の改竄が行われた場合の修正手順の概略を説明する。コンテンツの作成者は、クライアントコンピュータ７を使用して前記コンテンツを作成したものとする。前記作成者は作成したコンテンツ、即ちドキュメントファイル6a及びイメージファイル6bを従来と同様にして、開示すべきロケーションのサーバコンピュータ11の記憶装置12へ登録する。次に、同じコンテンツを改竄修正装置の実施に使用するサーバコンピュータ１の記憶装置２へ登録する。サーバコンピュータ１はアクセス許可を要求するユーザ（作成者）を情報提供者として認証したときのみ、コンテンツの登録要求を受け付ける。そして、改竄判定の対象とするコンテンツの開示先のロケーション等の監視設定を受け付けて登録する。

【００１９】サーバコンピュータ１は、登録されたロケーションからコンテンツを定期的に入手して、その内容が登録されたコンテンツと一致するか否かを判定する。一致しないと判定された場合、内容が改竄されているものと判断して、登録されたコンテンツを前記ロケーションへ開示する。これによって、改竄された内容が修正される。

【００２０】二つのコンテンツの内容が一致するか否かを判定するための最も単純な方法として、二つのコンテンツ（ファイル）の同じアドレスから取り出したデータを比較することが挙げられる。しかし、本発明の改竄修正装置においては、その判定のためにメッセージダイジェストを使用する。メッセージダイジェストとは、元のデータ（たとえば、通信文）からデータの指紋とも呼ぶべき特徴的なビットパターンを抽出する技術であって、例えば電子署名を実現するうえで欠かすことができない技術である。前記ビットパターンのサイズは、通常は固定長であって、その抽出には一方向関数であるメッセージダイジェスト関数を使用する。一方向関数とは、順方向に計算することは容易であるが、逆方向に計算することは非常に困難であるという性質を持った関数であって、例えばハッシュ関数がこれに該当する。

【００２１】メッセージダイジェスト関数は、前述の一方向関数の性質に加えて以下に示す二つの性質、

１．同じビットパターンが得られる二つの元データを見つけることが困難であること

２．ある特定のビットパターンを抽出できるような元データを見つけることが困難であること

を持った関数である。これらの性質はCollision Proof性と呼ばれる。

【００２２】あるデータ及び該データの内容保証が保たれた状態におけるメッセージダイジェストが与えられた状況において、データが改竄されているか否かを判定する場合、与えられたデータのメッセージダイジェストを抽出する。そして、抽出したメッセージダイジェストと与えられたメッセージダイジェストとを比較して、両者が一致しないとき、データが改竄されていると判定することができる。本発明の改竄修正装置においては、登録されたコンテンツのメッセージダイジェストと入手したコンテンツから抽出したメッセージダイジェストとを比較することによって、二つのコンテンツの内容が一致するか否かを判定する。

【００２３】

【発明の実施の形態】図１は、本発明に係る改竄修正装置の構成を示すブロック図である。図において、1aはCPU（Central Processing Unit）である。CPU 1aは、ネットワーク間の通信を制御する通信制御部1b，日付及び時刻を特定するカレンダ時計1c，経過時間を計時するタイマ1d，ワークメモリ1e及び記憶装置２とバス接続してある。通信制御部1bはファイアウォール３と接続している。

【００２４】図２は前記改竄修正装置におけるコンテンツの登録手順を示すフローチャートである。アクセス許可を要求するユーザの認証が成功したか否かを判別して(S1)、成功しなかったとき、処理を終了する。ユーザの認証が成功したとき、コンテンツの登録を受け付ける(S2)。そして監視すべきコンテンツの開示先のロケーション等の監視設定の入力を受け付けて、その設定情報を監視テーブル2cへ登録する(S3)。設定情報の登録を完了すると、タイマ1dへ所定の経過時間を設定して、計時を開始させる(S4)。

【００２５】図３は前記改竄修正装置におけるコンテンツの改竄判定及び改竄修正の手順を示すフローチャートである。監視テーブル2cに登録されたコンテンツが存在するか否かに基づき監視対象の有無を判別して(S11)、監視対象が存在しないとき、処理を終了する。S11にお

いて監視対象が存在するとき、タイマ1dによって計時した経過時間が所定時間に達したか否かを判別する(S12)。所定時間に達していないとき、S11へ処理を戻して、以降の手順を繰り返す。

【００２６】S12において、経過時間が所定時間に達したとき、監視テーブル2cに登録されたロケーションから監視対象のコンテンツを入手する(S13)。そして更新日付が登録されたコンテンツのそれと一致するか否かを判定して(S14)、一致するとき、同様にサイズが一致するか否かを判定する(S15)。サイズが一致するとき、内容が一致するか否かを公知のメッセージダイジェストによって判定して(S16)、一致するとき、以上の改竄判定処理に係る時刻、例えばコンテンツの入手時刻又は更新日付一致の判定時刻等を監視テーブル2cへ登録して(S17)、処理を終了する。

【００２７】S14において更新日付が一致しないとき、またS15においてサイズが一致しないとき、更にまたS16において内容が一致しないとき、記憶装置２に登録されているコンテンツ、即ちドキュメントファイル2a及びイメージファイル2bを前記ロケーションへ開示する(S18)。こうすることにより、開示先のロケーションに存在する改竄されたコンテンツが記憶装置２に登録されている元のコンテンツに修正される。そして、そのコンテンツの作成及び管理に関係するユーザへ、修正を行ったことを通知する電子メールを発信する(S19)。電子メールの発信を完了すると、S17へ処理を移して、改竄判定処理に係る時刻を登録し、処理を終了する。

【００２８】

【発明の効果】以上の如き本発明の改竄修正方法，改竄修正装置及び改竄判定装置によっては、情報提供者が行うべき監視操作を代行することによって、情報提供者であるユーザに多大な負担を強いることなく改竄操作を早急に関知するため、改竄による被害規模の拡大を抑止することができる。また、改竄操作を関知したときに、情報提供者が行うべき修正操作を代行して元の状態に修正するため、情報提供者であるユーザの操作負担を軽減することができる。

【図面の簡単な説明】

【図１】本発明に係る改竄修正装置の構成を示すブロック図である。

【図２】改竄修正装置におけるコンテンツの登録手順を示すフローチャートである。

【図３】改竄修正装置におけるコンテンツの改竄判定及び改竄修正の手順を示すフローチャートである。

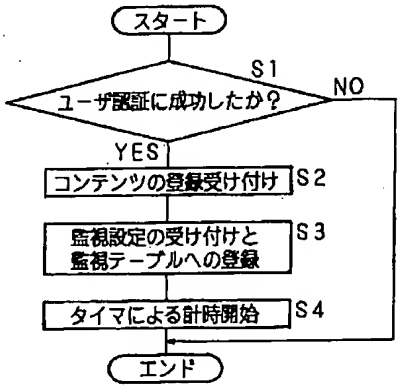
【図４】改竄修正装置を使用した改竄修正の概念を説明する説明図である。

【符号の説明】

1a　CPU
1b　通信制御部
1c　カレンダ時計
1d　タイマ
1e　ワークメモリ
２　記憶装置
2c　監視テーブル
３　ファイアウォール

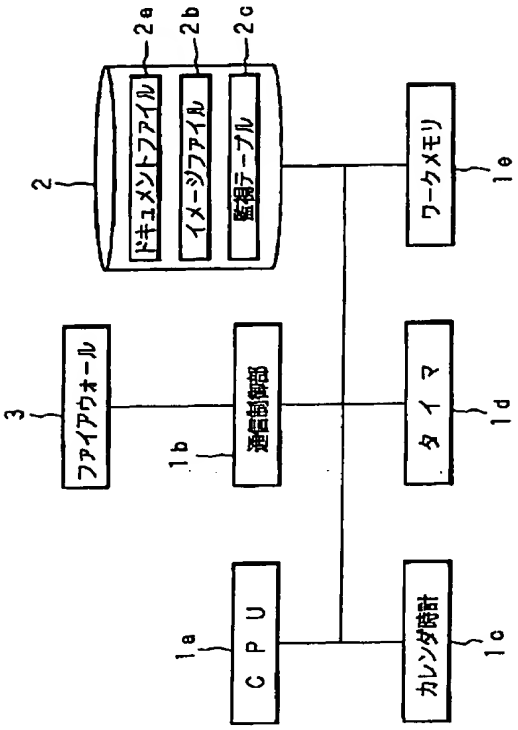
【図２】

改竄修正装置におけるコンテンツの登録手順を示すフローチャート



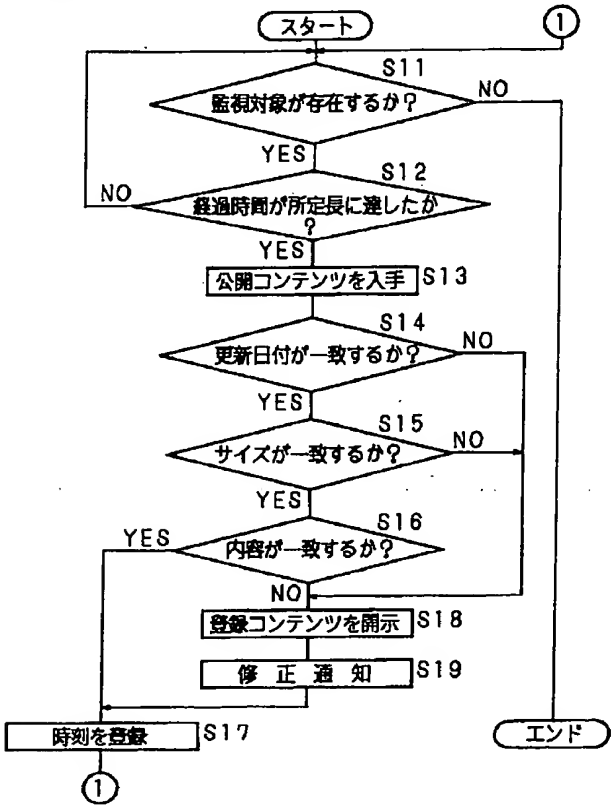
【図１】

本発明に係る改竄修正装置の構成を示すブロック図



【図３】

改竄修正装置におけるコンテンツの改竄判定及び改竄修正の手順を示すフローチャート



【図４】

改竄修正装置を使用した改竄修正の概念を説明する説明図